



Department of Homeland Security Daily Open Source Infrastructure Report for 23 March 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- Department of Homeland Security Secretary Chertoff has called for government regulation of chemical plant security, but said the industry should come up with its own protective measures, to be verified by private auditors. (See item [8](#))
- The Associated Press reports high levels of a radioactive material were found in groundwater near the Hudson River beneath New York's Indian Point complex, about 30 miles north of Manhattan. (See item [23](#))
- The Associated Press reports the nation's schools are being told to plan for the possibility of an outbreak of bird flu, and the government has created checklists on preparation and response steps. (See item [36](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *March 22, Associated Press* — **China, Russia seek more oil cooperation.** Russia and China pledged Wednesday, March 23, to cooperate more closely in producing oil and gas, and the Russian president vowed to go forward with a much-anticipated pipeline to carry Siberian oil to fuel China's booming economy within five years. However, Russian President Vladimir

Putin announced no details of the oil pipeline or its timing after meeting in Beijing with his Chinese counterpart, Hu Jintao. Russian officials say a feasibility study must be finished before those plans are finalized. Nevertheless, Wang Shengzi of state-owned China National Petroleum Corp. (CNPC) said the pipeline should be completed by about 2008 and carry 200,000 barrels of oil a day. Also Wednesday, the head of Russian oil company OAO Rosneft said it would launch joint ventures with CNPC to produce Russian crude and operate filling stations in China. China is lobbying for access to Russian oil and gas amid a worldwide scramble to secure energy for its sizzling economy, which grew nine percent last year.

Source: http://www.mercurynews.com/mld/mercurynews/business/financial_markets/14158055.htm

2. *March 21, Associated Press* — **Seattle City Light power lines threatened by sagging hillside.** A sagging hillside along Washington 530 between Arlington and Darrington, WA, is threatening some of Seattle City Light's main power lines. A collapse could take out metal towers that carry four high-voltage lines from Ross Dam to Seattle. City Light crews have installed large structures on either side of the highway to support the wires. The power lines carry nearly a third of the city's electricity, but utility spokesperson Dan Williams says that even if they go down an outage is unlikely because the utility would buy electricity on the open market.
Source: http://www.kirotv.com/news/8161981/detail.html?rss=sea&psp=n_orthsoundnews
3. *March 21, Associated Press* — **Gang allegedly eyed British bombings.** Suspected terrorists planning attacks in Britain were considering bombing nightclubs, trains, or the country's power network, and were in the final stages of the al Qaeda linked plot when they were arrested, a prosecutor said Tuesday, March 21. The seven defendants — all British — were caught in anti-terror raids in and around London in March 2004, during which police seized 1,300 pounds of ammonium nitrate fertilizer used for homemade bombs — about one-third the amount used in the 1995 Oklahoma City bombing that killed 168 people. Members of the group had previously flown to Pakistan for instruction at terrorist training camps and received backing from a senior al Qaeda operative, prosecutor David Waters said at the start of their trial. The defendants, who have pleaded not guilty, are accused of having acquired ammonium nitrate and aluminum powder "for bombs to be used in destructive attacks in the United Kingdom," Waters said. One defendant had worked at a company responsible for maintaining Britain's gas and electric infrastructure, a fact that was "of significance in this case," the prosecutor said.
Source: http://news.yahoo.com/s/ap/20060321/ap_on_re_eu/britain_bomb_plot_1
4. *March 20, Energy Business Review* — **Gazprom and Petro-Canada: Baltic terminal project hints at global LNG potential.** The Russian gas giant Gazprom and Canadian major Petro-Canada, one of Canada's largest integrated oil and natural gas companies, have signed an agreement to proceed with plans to build a gas liquefaction plant near St. Petersburg on the Baltic coast. The terminal should start operating in 2009 and will be able to bring long-term gas supplies to eastern Canada. Not only would Canadian customers potentially have an interest in LNG imports, but the U.S. too, where there has been an increase in LNG imports of 30 percent between 2003 and 2004, mainly being imported from Trinidad & Tobago.
Source: http://www.energy-business-review.com/article_feature.asp?gu_id=352DC119-A194-41F6-8C2A-98FD8C8304D1

5. *March 20, Reuters* — **Gasoline prices rise to highest level since late October.** The average price U.S. drivers paid for gasoline soared 13.8 cents, the third biggest weekly increase on record, to hit \$2.50 a gallon for the first time since last October, the Energy Information Administration (EIA) said on Monday, March 20. The national price for regular unleaded gasoline was up 40 cents from a year ago and the highest since October 24, based on EIA's survey of service stations. Gasoline costs have shot up 25 cents over the last three weeks as the spring driving season gets underway and some U.S. refineries are down due for maintenance. EIA analyst Tancred Lidderdale said U.S. gasoline inventories are near their highest levels in almost seven years and he was not aware of any major supply problems in the last week that would have caused the huge jump in pump prices. The EIA has said gasoline prices could rise in some U.S. markets this summer as refineries switch from making gasoline with the water polluting fuel additive MTBE to using corn-based ethanol.
Source: http://news.yahoo.com/s/nm/20060320/bs_nm/energy_gasoline_price_dc_1
6. *March 20, Bloomberg* — **New gasoline rules may trim importing.** U.S. refining capacity will rise in the next few years as gasoline imports decline from countries unable to meet new requirements for cleaner-burning fuel, said Joanne Shore of the Energy Information Administration. Speaking at the National Petrochemical and Refiners Association's annual meeting in Salt Lake City, UT, Shore said U.S. regulations have cut the sulfur content in gasoline and refiners this year are switching to an ethanol-blend fuel. Many sources of gasoline imports, including countries in Latin America and Eastern Europe, will no longer be able to produce gasoline that meets these requirements and domestic refiners will have to make up the shortfall, Shore said. Gasoline imports have met about half of domestic demand growth in the past 10 years, Shore said. Valero Energy Corp. Chief Executive Officer Bill Klesse said supplies of ethanol will be sufficient to meet demand this year. Demand for ethanol will rise by 130,000 barrels a day this year, according to an Energy Department report last month. Production may not rise fast enough to meet demand in the eastern U.S. and Texas.
Source: http://www.sltrib.com/ci_3622984?source=rss
7. *March 20, Houston Chronicle* — **Energy companies utilize Rita debris.** Six months after Hurricane Rita ravaged the East Texas piney woods, sawmills are stacked full with salvaged logs. But many communities are still littered with unsalvageable, splintered trees and waste wood from logging, such as branches and treetops. Michael Bishop, owner of an alternative power company in Nacogdoches, plans to collect the ruined wood and transform it into electricity for Europe. Bishop, president of American Biorefining, and Joe Murray of Green Energy Resources expect to collect millions of tons of shattered trees, branches and other forest debris. The pair plans to shred the waste wood into biomass fuel and ship it to European countries where such fuel is burned to generate power. Last year's tropical season, with hurricanes Katrina and Rita in August and September, respectively, gave him a bumper crop. He hopes to collect material from urban and suburban areas as well as forested lands. "This is just the beginning...There are several million tons in the general vicinity (of East Texas)," he said. Even without the hurricane damage, logging in East Texas forests generates about 2.8 million tons of "woody biomass" annually, said Burl Carraway of the Forest Service.
Source: <http://www.chron.com/disp/story.mpl/business/energy/3734464.html>

Chemical Industry and Hazardous Materials Sector

8. *March 21, Associated Press* — **Chertoff calls for chemical plant regulation.** Department of Homeland Security (DHS) Secretary Michael Chertoff called for government regulation of chemical plant security on Tuesday, March 21, but said the industry should come up with its own protective measures, to be verified by private auditors. Speaking at a forum hosted by the chemical industry, Chertoff said Congress needs to quickly give his department regulatory authority to bolster facilities that are attractive targets for terrorists. Chertoff said he envisioned performance standards, set by DHS, for chemical companies to follow. Those standards would not require specific safeguards, such as gates and guards, but would force the industry to develop adequate security plans at all manufacturing and storage facilities. Those standards could be validated by private auditors contracted with DHS, Chertoff said. Chertoff's remarks: <http://www.dhs.gov/dhspublic/display?content=5494>
Source: <http://www.cnn.com/2006/POLITICS/03/21/chemicalplant.securit y.ap/>

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report.

[\[Return to top\]](#)

Banking and Finance Sector

9. *March 21, Websense Security Labs* — **Phishing alert: Royal Bank of Scotland.** Websense Security Labs has received reports of a new phishing attack that targets customers of Royal Bank of Scotland. Users receive a spoofed e-mail message, which claims that their account information needs to be verified due to new security measures. The message provides a link to a phishing Website. Users who visit this Website are prompted to enter personal and account information.
Source: <http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =448>
10. *March 21, CNET News* — **Iowa proposes ID theft passport.** Lawmakers in Iowa are proposing a special "passport" meant to protect victims of identity theft against false criminal action and credit charges. The "Identity Theft Passport" will be a card or certificate that victims of identity fraud can show to police or creditors to help demonstrate their innocence, Tom Sands, a state representative of the Iowa House and supporter of the proposal, said. The passport can be presented to law enforcement officials to help prevent arrest or detention for an offense committed by someone using the victim's identity, according to the text of the bill proposing the measure. Also, victims could show it to creditors to help in any investigation and establish whether there has been any fraud, according to the proposal.
Source: http://news.zdnet.com/2100-1009_22-6052308.html
11. *March 21, KTUL NewsChannel 8 (OK)* — **ID theft of a different kind.** The latest version of identity theft is popping up as people are being asked to pay taxes on money someone else is making. The scam works such that after a thief steals someone's identity, they get a job on a

contract basis. The Internal Revenue Service thinks the person whose identity was stolen made the money and must pay the taxes. This time of year, this type of crime is being discovered because 1099s begin showing up in mailboxes.

Source: <http://www.ktul.com/printarticle.hrb?a=p&f=n&s=312376>

12. *March 21, Chicago Sun–Times* — **U.S. sees increase in counterfeit bills.** According to Russell C. Collett of the Secret Service, the bleaching method is becoming more common in northern Illinois, which has seen a recent rise in counterfeiting. About 25 percent more counterfeit currency was passed in this region in 2004 than in 2003, compared with about 15 percent more nationally. It's easy to detect counterfeit \$20 bills that have been printed on bleached \$5 notes because they will have a portrait of Jackson, but a watermark of Abraham Lincoln and a security thread that says "USA FIVE," Collett said. He said businesses should visually inspect bills instead of relying on counterfeit detector pens they often provide to their clerks because the pens will make the same golden mark on counterfeit currency created with legitimate \$5 notes that have been bleached and reprinted as fake \$20s, \$50s, and \$100s. Chicago street gangs such as the Black Disciples have become active in counterfeiting, learning the basics from prison contacts and fellow gang members on the street, Collett said. Not all gang members are using the bleaching method, however. Some phony money is made on an ink–jet printer and does not have any of the security features on genuine currency, authorities say.

Source: http://www.suburbanchicagonews.com/heraldnews/city/4_1_JO21_FAKE_S1.htm

13. *March 21, ZDNet Australia* — **Seek targeted by phishing campaign.** Online job site Seek has become the latest victim of a phishing campaign, with an e–mail circulating that attempts to gather confidential details from advertisers. Tam Vu, Seek's chief information officer, said that the phishing attack was launched at the end of last week. Vu said that he does not believe any of Seek's users have been duped into divulging their details. A contributing factor to the apparent failure of this particular attack could be that the phishing e–mail is poorly worded. The e–mail links to a bogus site mimicking Seek that attempts to collect usernames and passwords.

Source: http://www.zdnet.com.au/news/security/soa/Seek_targeted_by_phishing_campaign/0.2000061744.39246967.00.htm?feed=rss

[\[Return to top\]](#)

Transportation and Border Security Sector

14. *March 22, Associated Press* — **EU bans 92 airlines from landing at European airports.** The European Union (EU) on Wednesday, March 22, banned 92 airlines, most of them based in Africa, from landing at European airports, declaring them unsafe by international standards. The ban applies to cargo and passenger carriers from Congo, Equatorial Guinea, Sierra Leone, Swaziland, and Liberia judged to have an "inadequate system for regulatory oversight" or insufficient safety standards. It will be enforced by all 25 EU nations, plus Norway and Switzerland. EU Transport Commissioner Jacques Barrot said the EU was barring 50 carriers from Congo alone, 14 from Sierra Leone and seven from Swaziland, virtually ensuring that all airlines operating from those countries were prevented from flying to Europe. He said some planes used for flights to Europe and possibly elsewhere were "flying coffins," adding that

safety controls in the listed nations were too weak. The EU moved to set up a single list after several fatal airline crashes in Greece and Italy last year and the fatal crash of Egypt's Flash Airlines in the Red Sea in June 2004, which killed 148 people, mostly French tourists. Barrot said the EU would also provide aid to African nations in trying to upgrade airline safety standards.

Source: http://www.usatoday.com/travel/flights/2006-03-22-eu-blacklist_x.htm

15. *March 22, Associated Press* — **Hawaiian Holdings posts loss.** Hawaiian Holdings Inc., parent of Hawaiian Airlines, on Wednesday, March 22, posted a wider fourth-quarter loss due to increased fuel costs and an unusually hefty income tax provision. The company, which emerged in June from Chapter 11 bankruptcy, posted a loss of \$19.5 million, or 43 cents per share, compared with a loss of \$1.7 million, or 5 cents per share, in the prior-year period. Fuel costs increased 49 percent to \$59.8 million in the quarter. Total operating expenses were up 22 percent to \$220.6 million.

Source: http://biz.yahoo.com/ap/060322/earns_hawaiian_holdings.html?_v=1

16. *March 22, Idaho Statesman* — **FAA plan for airport on hold.** The Federal Aviation Administration (FAA) has put a temporary hold on plans to move part of Boise, ID, Airport's air-traffic control system to Salt Lake City, observers said Tuesday. Instead, FAA officials will try to address concerns raised by the proposal during a meeting Thursday, March 23, with airport administrators, according to an agency spokesperson. The FAA reportedly wants to move the Terminal Radar Approach Control system — or TRACON — currently located at Boise Airport to Salt Lake City in hopes of saving \$5 million on the proposed \$22 million cost of a new air-traffic control tower in Boise. The TRACON is the part of the three-tiered air traffic control system that ensures that departing planes are on course and at safe altitudes, and that arriving traffic is properly positioned to land. An internal FAA study in 2005 showed that Boise Airport was one of 15 facilities scheduled to have its TRACON relocated this year. Critics of the move say moving the TRACON could result in higher operating costs for commercial and private air traffic, produce higher ticket prices for air travelers and potentially represent safety hazards because a Salt Lake City TRACON would be monitoring 30 miles of Boise air space from a location 300 miles away.

Source: <http://www.idahostatesman.com/apps/pbcs.dll/article?AID=/20060322/NEWS02/603220315/1029>

17. *March 22, Seattle Times* — **Alaska inspection finds no cabin-pressure flaws.** Alaska Airlines has completed an inspection of the pressurization systems on all 112 airplanes in its fleet and has found no pervasive flaws or weaknesses that could trigger an unexpected loss of cabin pressure. "We completed those inspections Sunday, March 19, and they confirmed there are no systemic issues with our pressurization systems," said Amanda Tobin, an Alaska spokesperson. The Seattle-based airline began the inspection last month, after a span of 10 days in which five airplanes encountered in-flight problems with their pressurization systems. The incidents not only involved five different airplanes, but also a mix of MD-80 and 737 models of varying age. Alaska said at the time that its initial investigation of the incidents had uncovered no common root cause.

Source: <http://archives.seattletimes.nwsource.com/cgi-bin/taxis.cgi/web/vortex/display?slug=alaska22&date=20060322&query=airline>

18. *March 17, Reuters* — **JetBlue adds U.S. routes in effort to boost sales.** JetBlue Airways Corp. looking for ways to revive its fortunes after a recent spate of bad news, said on Friday, March 17, it would begin flying two routes where there is limited competition. The routes to Pittsburgh will use JetBlue's 100-seat Embraer 190 jets. The airline has been trying to prove that adding the Brazilian-made planes as a second fleet type alongside its existing Airbus A320 planes was the right move. The E-190s, which began flying last year, got off to a rocky start as they were plagued by reliability issues, and the airline pulled back some of its planned expansion for the jets. JetBlue Chief Executive David Neeleman earlier this week said the airline would seek routes on which there was limited competition as it looks to raise ticket prices. He also said the reliability issues with the E-190s were mostly resolved.
Source: http://biz.yahoo.com/rb/060317/airlines_jetblue.html?.v=1

[[Return to top](#)]

Postal and Shipping Sector

19. *March 22, Atlanta Business Chronicle* — **UPS Trade Direct service grows.** United Parcel Service Inc. (UPS) has begun its Trade Direct service for exports from the United States and Canada to Europe. UPS said its Trade Direct service will help customers in the U.S. and Canada ship goods faster and more efficiently to Europe, while ending the need for client distribution centers in the receiving country for breaking apart freight shipments.
Source: <http://biz.yahoo.com/bizj/060322/1262470.html?.v=1>

[[Return to top](#)]

Agriculture Sector

20. *March 22, USAgNet* — **Soybean fungus hunt to focus on Southern states.** The U.S. Department of Agriculture (USDA) monitors movements of Asian soybean rust by coordinating with states to regularly check selected fields, or sentinel plots, scattered across the eastern half of the country. The USDA is increasing the number of sentinel plots that it pays for to 349 this year, up 18 from last year, and concentrating on new sites in Southern states where the fungus has been found. Florida will have 30 USDA-funded sentinel plots this year, compared with 15 last year. Louisiana will have 25, up from 15. Mississippi and Alabama will have 25 and 22 respectively, compared with 24 and 10 last year.
Source: <http://www.usagnet.com/story-national.cfm?Id=461&yr=2006>

21. *March 22, Agricultural Research Service* — **Genetic tests may improve cattle breeding.** Geneticists with the Agricultural Research Service (ARS) are improving traditional cattle breeding methods with marker-assisted selection, a process that incorporates DNA tests into traditional genetic evaluation systems. Traditionally, breeders have used visual appraisal to estimate cows' genetic merit. By carefully recording the characteristics of herd members and their descendents, animal breeders can calculate an animal's Expected Progeny Difference (EPD). This is a figure estimating the average performance of specific traits for an individual's offspring. More recently, geneticists have developed DNA tests associated with important traits in cattle. These tests might someday be incorporated into the established selection process.

According to ARS geneticist R. Mark Thallman, incorporating DNA tests in breeders' calculations could improve the accuracy of their EPDs and place the appropriate degree of emphasis on the DNA tests. With geneticist Mark F. Allan, he is testing that theory, using a herd selected for producing twins as a prototypical population. Previous research located three genetic regions linked to the twinning trait. In similar work, researchers from Cornell University, ARS, and Iowa State University incorporated DNA test results into a genetic evaluation of Simmental cattle for tenderness, allowing Simmental breeders to use marker-assisted selection for tenderness.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

22. *March 22, News-Press (FL)* — **Citrus greening found in Cape.** Just when citrus growers thought it was safe to replant their trees, an even deadlier disease has cropped up in Lee, Fl. State agriculture officials have confirmed a case of citrus greening at a residence in northwest Cape Coral. The discovery comes two weeks after the Florida Department of Agriculture gave residents the permission to replant the more than 30,000 trees lost to citrus canker. Local growers are being urged not to replace their citrus trees because of the newest threat. Unlike canker, which can be detected almost immediately after it has infected a tree, greening symptoms are often mistaken as a simple nutrition deficiency. Three to five years may pass before an infected tree shows the deadly signs. In most cases, trees are dead in fewer than eight years. Greening has been killing trees on the east coast of Florida since it was first discovered in Homestead in August. Now, 240 trees are infected in 12 counties, and its westward movement has citrus industry leaders very concerned.

Citrus greening information: <http://ipm.ifas.ufl.edu/agricultural/fruit/citrus/ASP-hoy.htm>

Source: <http://www.news-press.com/apps/pbcs.dll/article?AID=/20060322/NEWS0101/603220419/1075>

[[Return to top](#)]

Food Sector

Nothing to report.

[[Return to top](#)]

Water Sector

23. *March 21, Associated Press* — **High level of radioactive material in water.** High levels of a radioactive material were found in groundwater near the Hudson River beneath a nuclear plant, the owner said Tuesday, March 21. The material was nearly three times the amount permitted in drinking water. The groundwater does not reach drinking supplies, and although the strontium-90 is believed to have reached the Hudson it would be safely diluted in the river, said Jim Steets, spokesperson for Entergy Nuclear Northeast. The strontium — which can cause cancer in high doses — was found in a well dug in a search for the source of a leak of radioactive water at New York's Indian Point complex, about 30 miles north of Manhattan. The test well is among nine dug in an attempt to pinpoint the leak. Contaminated water was first found in August.

Source: <http://www.sunherald.com/mld/sunherald/14155493.htm>

Public Health Sector

24. *March 22, University of Wisconsin–Madison* — **Cell barrier slows bird flu's spread among humans.** Although more than 100 people have been infected with the H5N1 avian influenza virus, mostly from close contact with infected poultry, the fact that the virus does not spread easily from its human hosts to other humans has been a biomedical puzzle. Now, a study of cells in the human respiratory tract reveals a simple anatomical difference in the cells of the system that makes it difficult for the virus to jump from human to human. The finding is important because it demonstrates a requisite characteristic for the virus to equip itself to easily infect humans, the key development required for the virus to assume pandemic proportions. Experiments using tissue from humans showed that only cells deep within the respiratory system have the surface molecule or receptor that is the key that permits the avian flu virus to enter a cell. Flu viruses, like many other types of viruses, require access to the cells of their hosts to effectively reproduce. If they cannot enter a cell, they are unable to make infectious particles that infect other cells — or other hosts.

Source: <http://www.news.wisc.edu/12345.html>

25. *March 21, Agence France–Presse* — **Malaysia fears bird flu may spread nationwide.** A Malaysian deputy minister warned that the bird flu virus may spread nationwide after two more outbreaks were reported in a northern state. An official in the northern state of Perak reported two new outbreaks of the H5N1 strain there, at Changkat Legong and at Titi Gantung. In the first outbreak in Malaysia in more than a year, H5N1 was detected last month in 40 free-range chickens in four villages in Gombak near Kuala Lumpur. Thursday, March 16, Malaysia announced outbreaks of H5N1 in an eco-park and at Changkat Tualang. On Monday, March 20, an outbreak of H5N1 was announced in Permatang Bagak village in Penang state bordering Perak. Officials have slaughtered tens of thousands of birds at the site of outbreaks. No human cases of bird flu have been reported so far in the country.

Source: http://news.yahoo.com/s/afp/20060321/hl_afp/healthflumalaysia_060321163903;_ylt=AgiPOhX_87vyephNJmbEAlSJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--

26. *March 20, Angola Press* — **Strange disease kills ten people in Angola.** Ten people have died of a strange disease that broke out in mid-February 2006 in Tcholindi village, about 20 miles north of Mungo district, Angola's central Huambo province. The information was released by Tcholindi's chief, António Epalanga, who said he does not know the origin of the disease that attacks the legs before expanding to the intestines, killing the patient within less than a weeks time.

Source: <http://www.angolapress-angop.ao/noticia-e.asp?ID=426288>

Government Sector

27. *March 22, Reuters* — **Man held for tossing harmless package at White House.** A man was taken into custody after throwing a suspicious package over the White House fence on Wednesday, March 22, but no explosives were found, the Secret Service said. Tom Mazur, spokesperson for the Secret Service, said a similar incident had occurred before. Officials proceeded with bomb investigating procedures as a precaution though past incidents have not involved explosives. Police sealed off the front gates of the White House and a bomb squad converged on the area to investigate the object. Mazur said the package was thrown along the north fence line of the White House but was found to be harmless.

Source: http://www.boston.com/news/nation/washington/articles/2006/03/22/white_house_gates_sealed_due_to_suspicious_package/

[[Return to top](#)]

Emergency Services Sector

28. *March 22, Houston Chronicle* — **Houston area must quickly choose disaster commander.** Houston area judges and mayors have less than a month to select a single operational commander to coordinate evacuations and emergency response, Governor Rick Perry ordered Tuesday, March 21. The order, a result of Perry's efforts to improve upon last year's massive and troubled evacuation ahead of Hurricane Rita, seeks to better coordinate command and communications among numerous governmental agencies with often competing interests. The county judges and mayors within each of 24 "councils of government" in Texas must establish a command structure by April 18 and name an incident commander by April 20. The local region, known as the Houston–Galveston Area Council, encompasses Harris and 12 surrounding counties. The governor's order came after an evacuation task force convened in Rita's aftermath completed its report last month. The panel's chief recommendations were to improve communication and decision making during crises. Officials hope to avoid the logistical and other problems that result when multiple cities, counties and regional jurisdictions must reach timely decisions in staging and managing evacuations.

Source: <http://www.chron.com/disp/story.mpl/front/3739709.html>

[[Return to top](#)]

Information Technology and Telecommunications Sector

29. *March 22, Herald Sun (Australia)* — **Man arrested over online attacks.** A man charged with over a series of high–profile international Internet hacking attacks was arrested in Melbourne, Australia, early Wednesday, March 22, after a joint state and federal investigation into the sophisticated attacks on Internet relay chat servers in Australia in 2005. The Belgian Federal Computer Crime unit tipped Australian authorities off to the attacks, which used botnets.

Source: http://www.heraldsun.news.com.au/common/story_page/0,5478,18562814%5E661,00.html

30. *March 22, U.S. Computer Emergency Readiness Team* — **US–CERT Technical Cyber Security Alert TA06–081A: Sendmail race condition vulnerability.** A race condition in Sendmail may allow a remote attacker to execute arbitrary code. Sendmail contains a race

condition caused by the improper handling of asynchronous signals. In particular, by forcing the SMTP server to have an I/O timeout at exactly the correct instant, an attacker may be able to execute arbitrary code with the privileges of the Sendmail process. Systems affected:

Sendmail versions prior to 8.13.6.

Solution: Upgrade Sendmail: Sendmail version 8.13.6 has been released to correct this issue:

<http://www.sendmail.org/8.13.6.html>

Patches to correct this issue in Sendmail versions 8.12.11 and 8.13.5 are also available.

Version 8.12.11: <ftp://ftp.sendmail.org/pub/sendmail/8.12.11.p0>

Version 8.13.5: <ftp://ftp.sendmail.org/pub/sendmail/8.13.5.p0>

Source: <http://www.uscert.gov/cas/techalerts/TA06-081A.html>

31. *March 21, Security Focus* — Macromedia Flash multiple unspecified security

vulnerabilities. The Macromedia Flash plug-in is susceptible to multiple unspecified vulnerabilities. Analysis: Critical vulnerabilities have been identified in Flash Player that could allow an attacker who successfully exploits these vulnerabilities to take control of the affected system. A malicious SWF must be loaded in Flash Player by the user for an attacker to exploit these vulnerabilities. Users are recommended to update to the most current version of Flash Player available for their platform. A complete list of vulnerable products is listed in the source advisory.

Solution: Adobe has issued advisory APSB06-03 along with fixes to address these issues. See the following references for more details: <http://www.securityfocus.com/bid/17106/references>

Source: <http://www.securityfocus.com/bid/17106/info>

32. *March 21, eWeek* — Spyware trail leads to Kazaa, big advertisers. The StopBadware.org coalition, funded by Google, has listed the Kazaa file-sharing application at the top of a list of noxious software programs that present a threat to business and consumer users. The coalition, which counts Sun Microsystems and Lenovo among its sponsors, will recommend in its inaugural Badware Report that users stay away from Kazaa and three other programs that can be combined with Trojans and bots for use in data theft attacks. Adware and spyware programs that come bundled with peer-to-peer applications present a huge security risk to corporate networks, and StopBadware.org says Kazaa's claim to be spyware-free cannot be trusted. In addition to Kazaa, StopBadware.org said computer users should stay away SpyAxe, a rogue anti-spyware program; MediaPipe, a download manager that offers access to media content; and Waterfalls 3, a screensaver utility.

StopBadware.org Report: <http://www.stopbadware.org/pdfs/badwarev1r3.pdf>

Source: <http://www.eweek.com/article2/0.1895.1940747.00.asp>

33. *March 21, Federal Computer Week* — Michigan unveils long-term IT strategic plan.

Michigan state government officials unveiled Tuesday, March 21, a new strategic information technology plan that sets goals and targets to improve access to services, foster collaboration across agencies and other communities, make government more efficient, and attract and retain employees. The 209-page plan — including 12 appendices on different IT subjects — is focused on improving education, homeland security, health care, government, the economy and the environment by establishing specific targets and metrics for several strategies.

Source: <http://fcw.com/article92679-03-21-06-Web>

34.

March 21, Tech Web — **China reportedly says it will block some VoIP calls.** China says it will block computer-to-landline phone service for two years, in order to protect its own local telephone services, it was reported Tuesday, March 21. Beijing will not issue voice over Internet protocol licenses until 2008.

Source: <http://www.techweb.com/wire/networking/183701638>

- 35. *March 21, IDG News Service* — Researchers warn of Trojan hearse.** Security researchers at Sana Security Inc. are warning of a new type of malicious software designed to steal usernames and passwords from Web surfers. The malware, dubbed "rootkit.hearse," uses rootkit cloaking techniques, making it extremely difficult to detect. In order to steal information, however, the software must first be downloaded onto a user's system. This can be done by tricking the user into downloading the malicious code, or by infecting a computer with some other form of malware. Once installed, it sends the sensitive information to a server in Russia, that appears to have been in operation since Thursday, March 16, Sana said.

For more information on rootkit hearse:

http://www.nthworld.org/archives/2006/03/on_march_20th_w.htm

Source: http://www.infoworld.com/article/06/03/21/76669_HNtrojanhearse_1.html?source=rss&url=http://www.infoworld.com/article/06/03/21/76669_HNtrojanhearse_1.html

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT is aware of several vulnerabilities in Adobe Macromedia Flash products. A system may be compromised if a user accesses a web page that references a specially crafted Flash (SWF) file. Successful exploitation may allow a remote attacker to execute arbitrary code with the privileges of the user. For more information please review the following:

VU#945060 – Adobe Flash products contain multiple vulnerabilities

<http://www.kb.cert.org/vuls/id/945060>

TA06-075A – Adobe Macromedia Flash Products Contain Vulnerabilities

<http://www.us-cert.gov/cas/techalerts/TA06-075A.html>

Adobe Security Bulletin: APSB06-03

http://www.macromedia.com/devnet/security/security_zone/apsb_06-03.html

Microsoft Security Advisory: 916208

<http://www.microsoft.com/technet/security/advisory/916208.mspx>

US-CERT encourages administrators to apply the appropriate updates, patches, or

fixes as soon as possible.

Current Port Attacks

Top 10 Target Ports	1026 (win-rpc), 80 (www), 6881 (bittorrent), 113 (auth), 445 (microsoft-ds), 41170 (---), 139 (netbios-ssn), 1027 (icq), 25 (smtp), 32459 (---)
----------------------------	---

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

36. *March 22, Associated Press* — **Schools told to prepare for bird flu.** The nation's schools, recognized incubators of respiratory diseases among children, are being told to plan for the possibility of an outbreak of bird flu, the name for the deadly H5N1 strain of the avian flu. School boards and superintendents have gotten used to emergency planning for student violence, terrorism or severe weather. Pandemic preparation, though, is a new one. In North Carolina on Tuesday, March 21, Education Secretary Margaret Spellings joined Health and Human Services Secretary Mike Leavitt to encourage schools to prepare. Spellings said schools must be aware that they may have to close their buildings — or that their schools may need to be used as makeshift hospitals, quarantine sites or vaccination centers. The government has created checklists on preparation and response steps, specialized for preschools, grade schools, high schools and colleges. The dominant theme is the need for coordination among local, state and federal officials. At the college level, the American Council on Education, a higher education umbrella group, has alerted thousands of college presidents about the need to prepare for bird flu. Federal health leaders have advised each college to establish a pandemic response team and plan for outbreak scenarios that could close or quarantine their campuses.

Source: <http://www.breitbart.com/news/2006/03/22/D8GGKFE00.html>

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.